

アシュアランスマップを活用した グループガバナンスの高度化

PwCあらた有限責任監査法人
ガバナンス・内部監査部門
パートナー 高木 和人



はじめに

本年6月に改訂されたガバナンスコードによると、取締役会を中心にグループ全体のリスク管理体制を整備し、内部監査を活用して運用状況を監督することが必要とされています。また、社外取締役は、海外子会社を中心にリスク管理の脆弱性を指摘し、グループガバナンスの実質的な高度化を求めています。投資家も予測不能な環境下において、レジリエントなリスク管理体制に着目しており、企業に対して積極的な開示と継続的な対話を要求しています。

このような社会の要請に対して、外部環境の変化がより一層速くなり、自社が管理するリソースの境界が曖昧で複雑化していることから、グループ全体のリスク管理体制に自信を持ってない経営者が増えていると思われます。そこで本稿では、アシュアランスマップを活用してグループガバナンスの高度化に取り組んだ事例を紹介し、注意すべきポイントについて解説します。

なお、文中の意見に係る部分は筆者の私見であり、PwCあらた有限責任監査法人または所属部門の正式見解ではないこと、あらかじめご理解頂ければと思います。

1 アシュアランスマップ作成の目的

子会社からリスク情報を収集する仕組みが本社事業部門やコーポレート部門によって整備されておらず、管理状況もモニタリングできていない結果、グループ全体のリスク管理の状況を十分に把握できていない会社を目にします。また、内部監査に対する投資が十分でなく、リスク管理の強化によるグループガバナンスの継続的な高度化に取り組めていない会社もあります。

このような状況を改善するために、グループにとって重大なリスクとそれに対応するアシュアランス活動を整理することが作成の目的となります。具体的には、縦軸に企業グループにとって重大なリスクを記載し、横軸には3ラインを中心とした内外のアシュアランス活動を記載することで、リスクへの対応が見える化し、経営判断に資する情報を提供することが目的となります（後述の図表1を参照）。

3ラインモデル

第1線の役割は、顧客に対する価値の提供と現場での最前線のリスク管理を行うことです。第1線が機能するように、専門性を活かして現場への指導やモニタリングを行い、重大なリスクが顕在化しないように支援するのが、第2線の役割です。また、第3線は、第1線と第2線のリスク対応状況を確認する内部監査の役割で、課題を発見して改善を促すことで、全社最適なリスク管理体制をアシュアランスする機能を果たしています。

3ラインモデルを車の運転にたとえると、第1線は運転手であり、アクセルを踏んで収益機会を探索し、時にはブレーキをかけて損失を回避します。道路状況や天候等の外部環境を踏まえてアクセルとブレーキを使い分

けることは、まさにビジネスそのものであり、リスクオーナーである運転手は最前線でリスクを管理します。一方、第2線は、助手席に座って運転手を支援する専門家で、時にはアクセルを踏むことや安全運転を促すことで大きな事故から守ります。第3線は、第1線と第2線のリスク対応の状況を後部座席から確認する役割で、運転手と助手席がしっかり連携していることを後部座席からアシュアランスします。

2 アシュアランスマップの作成方法

アシュアランスマップの作成方法や事例は、各社の目的によって異なっています。今回は、PwC英国が2021年1月にウェブサイトに掲載した「Exploring the Assurance Map」を参考に、6つのステップに分けた作成方法と作成例(図表1)について、日本での事例も加えながら紹介します。

6ステップによる作成例

- **ステップ1：主要なリスクを特定する**
リスクレジスターの中から、理想的には5～10程度の主要なリスクに絞って選定します。
- **ステップ2：リスクとコントロールを評価して残余リスクを特定する**
リスクに対応する内部統制、プロセスおよびガバナンスを特定し評価します(第1線と第2線)。
- **ステップ3：リスクと関連するアシュアランス提供者を特定し、潜在的なギャップを識別する**
プロセスやコントロールに対する内部(第3線)と外部のアシュアランス活動に着目します。
- **ステップ4：リスクと関連するKPI(Key Performance Indicator)や公開情報を確認する**
各リスク領域に関連するKPIが公開されている場合には、アシュアランスマップに記載します。
- **ステップ5：KPIと関連するアシュアランス活動を特定し、潜在的なギャップを識別する**
ステップ3と同様に、内部および外部のアシュアランス活動に着目します。
- **ステップ6：これまでのステップを踏まえて、残余リスクの状況を評価し、必要に応じてステークホルダーとの対話を行い、潜在的なギャップの有無を検討する**

取締役会や監査委員会は、残余リスクが十分に低減されているか検討し、さらなるコントロールの強化が必要か決定します。

重大なリスクに絞り込む

実務担当者の視点に立ってリスクを選定すると、網羅性を重視する結果リスクの粒度が細くなることがあります。また、有価証券報告書に記載されている「事業等のリスク」の情報を適用すると、各社横並びの記載から十分な効果が得られない場合もあります。これらを防ぐには、経営執行会議や取締役会が着目する特に重大なリスクに絞り込み、総花的な対応によってアシュアランスマップの作成が形骸化しないように注意することが必要です。さらに、管理体制の重大な課題を中心に分析し、経営判断に資する実践的なものとすることが重要です。

残余リスクの識別にはツールの活用が効果的

海外も含めたグループ全体の残余リスクを評価するステップ2は、実態を把握することが難しく、かなりの工数を要する取り組みです。しかし、クラウド環境に構築されたRCSA(Risk Control Self-Assessment)を活用すれば、リスクとコントロールを紐づけて評価し、本社から各拠点の残余リスクを効率的に評価できるようになります。

RCSAツールを利用すれば、各リモート拠点でメールのリンクにIDとパスワードを入力することで、リスクとコントロールを同じ画面上で評価できます。また、同ツールのチャット機能を使えば、双方向のコミュニケーションをリモート環境下で行えるため、実態の正しい把握にも貢献します。さらに、コントロールに関連する文書を添付してもらえば、本社にいながら多数の拠点の文書をリモート環境で確認できるようになります。

リスクの種類は広く捉える

各社の目的によって異なりますが、オペレーショナルリスクやコンプライアンスリスクのうち、重要なものに絞って分析している会社もありますが、これは、取締役の責任である内部統制の構築と3ラインによる管理が、紐づけて分析しやすいことが背景にあると思われます。

しかし、予測不能な環境下においては、内外の環境変化、戦略リスクおよびESGに関連する時間軸の長いリスク等、グ

ループ本社が中心となって個別にトップダウンで対応することが効果的なリスクが増えています。投資家も、変化の激しい時代において、対話の対象となるリスクの種類をビジネスと紐づけて幅広く捉えることを求めています。したがって、取締役や投資家の視点に立った場合、重要なリスクに数は絞った上で、リスクの種類はあまり限定せず、対象範囲を広く捉えることが望ましいと考えられます。

アシュランスマップの例示

アシュランスマップの作成例を図表1に挙げています。ここではリスクを非財務・規制リスク、オペレーションリスク、財務リスクおよび戦略リスクの4つに分類し、そのうち主要なリスクとして、ESGの影響、サイバー、資産計上されたソフトウェアおよびイノベーションの失敗をリスクレジスターから選定しています。

例えば、資産に計上されたソフトウェアの場合、発生可能

性と影響度から固有のリスクを「中程度」と評価し、年次の減損テスト等主要なコントロールの有効性を分析した結果、残余リスクも「中程度」としています。

そして、残余リスクの評価結果と、第3線である内部監査人と外部監査人のアシュランス活動を紐づけて確認します。具体的には、両監査人ともサンプルベースでコントロールテストを実施しており、外部監査人は年度末に減損テストも実施しているため、リスクが十分に低減されているか期待ギャップの有無も含めて確認します。同様に、リスク管理上の重要なKPI (Key Performance Indicator) の開示状況とアシュランス活動についても関連付けて分析します。アニュアルレポートにはROI (投資収益率)、帳簿価格および減損額が関連するKPIとして開示されているため、外部監査人による財務諸表計上額および関連するKPIのアシュランス活動について、期待ギャップの有無を確認します。これらの一連のリスク管理活動の十分性については、最終的に取締役

図表1：アシュランスマップの作成例

ステップ1： 主要なリスクを特定する		ステップ2： リスクとコントロールを紐づける			ステップ3： リスクと関連するアシュランス提供者を特定し、 潜在的なギャップを識別する	
既存のリスクレジスターから取り出された情報						
	リスクの内容	固有リスク (可能性と影響を考慮)	リスク対応 (第1線および第2線)	残余 リスク	リスクに対する内部ア シュランス (第3線)	リスクに対して提供される 外部アシュランス
非財務・規制	環境、社会、ガバナンス (ESG) への影響：企業が ESG でもたらす影響のネガティブな報道により、消費者が離れ、ブランド価値と業績低下につながる可能性	中程度	<ul style="list-style-type: none"> 取締役会によって承認された ESG に関する明確な方針 戦略に沿った方針やプロセス サプライヤー、製造業者および請負業者の承認済みリスト 業界に対するベンチマーキング 実行済みの対策に関する外部とのコミュニケーション 	中程度	—	—
オペレーション	サイバー：サイバー攻撃により、システムの停止、事業の中断、データの紛失やレピュテーションの低下につながる可能性	高い	<ul style="list-style-type: none"> ITの方針 サイバーリスクに対する内部統制 危機対応計画 ペネトレーションテスト リスクに関するスタッフの研修 	高い	年間を通じてサンプルベースによりコントロールの有効性を内部監査がテスト	—
財務	資産計上されたソフトウェア：資産計上されたソフトウェアへの投資が、当初の目的を果たせず、投資額を回収できない可能性	中程度	<ul style="list-style-type: none"> 新規ソフトウェアの承認、取得、開発に関する財務およびITコントロール 適切な権限の委譲 計画と実際の進捗レビュー 年次減損レビュー 	中程度	年間を通じてサンプルベースによりコントロールの有効性を内部監査がテスト	外部会計監査チームは、主要なコントロールの有効性をサンプルベースでレビューし、年度末に残高の回収可能性を評価
戦略	イノベーションの失敗：日々変化する消費者のニーズを満たす、革新的な製品やサービスへの投資、開発、提供に失敗した場合、事業の成長が妨げられ、業績に影響が出る可能性	高い	<ul style="list-style-type: none"> 消費者の嗜好やトレンドを把握するための継続的な市場調査・アンケート 専任のイノベーションチームによる、今後発売される新製品のテスト 新規事業の取得によるビジネスの多様化 既存サービスの継続的な影響に関する内部レビュー (競合他社および自社過年度との比較) 	高い	—	—

出所：PwC英国が作成したものを日本語に翻訳

<https://www.pwc.co.uk/audit-assurance/assets/pdf/assurance-map.pdf>

会や監査委員会によって決定されることになります。

3 残余リスクに応じた第2線の支援活動

グループにとって重大な残余リスクがある場合には、本社と子会社第2線が連携して、第1線のリスク管理体制を強化していくことが効果的です。本社第2線は、子会社第2線の成熟度に応じて、支援活動の強弱を検討します。子会社第2線の成熟度が高い場合には、子会社側にリスク管理体制の強化を任せたと上で、進捗をモニタリングするようにします。一方、子会社第2線が脆弱な場合には、本社第2線は子会社第2線と協働で第1線のリスク管理体制の強化にあたります。すなわち、本社第2線は、子会社で対応が必要なリスク管理の方針を提示し、プロセス、コントロールの整備やこれらが機能するように人材の育成を支援します。そして、モニタリ

ングの頻度を増やししながら、子会社第1線・第2線のリスク管理体制が強化され、残余リスクが許容可能な水準に下がるまで積極的に関与します。

不適切事案を繰り返す子会社は、第1線・第2線の管理体制が脆弱であるにもかかわらず、本社の関与も十分でなく、現場が閉鎖的な環境となっている場合があります。このような場合には、本社第2線も関与して現場プロセスの透明性を高め、モニタリング活動を通じた行動の変革を促すことで、風通しの良いリスクカルチャーの醸成を目指すのが効果的な方策となります。

ステップ4： リスクと関連するKPIや公開情報を確認する		ステップ5： KPIと関連するアシュアランス活動を特定し、潜在的なギャップを識別する	
リスクに関連するKPI やその情報	KPI / リスク領域 の報告書	KPI (第3線) に対して 現在提供されている 内部アシュアランス	KPI に対して現在提供され ている外部アシュアランス
<ul style="list-style-type: none"> 二酸化炭素排出量 水の使用量 最終埋立処分率 	アニュアルレポート、 サステナビリティレポ ートへの掲載	—	他のアシュアランス提供者 が、報告されたKPIに対 して、年次ベースで限定的 なアシュアランスを提供
n/a	IT部門は、期中に特 定されたサイバー問 題をまとめた月次報 告書を取締役会に提 出	n/a	n/a
<ul style="list-style-type: none"> 投資利益率 財務諸表に資産計 上されたソフトウェア の帳簿価額および償却額 	アニュアルレポートに 掲載	—	外部監査人は、資産計上 されたソフトウェア残高全 体に対するアシュアランス と関連するKPIには限定的 なアシュアランスを提供
<ul style="list-style-type: none"> 顧客調査 既存の製品ポート フォリオの有効性 ／影響 	会社ホームページに 掲載	—	

子会社の成熟度と権限の委譲

リスクが高く管理体制が脆弱な子会社に本社が関与しないことは、リスクの高い重要な業務を新入社員に一任している状況と似ています。新入社員に対しては、具体的な指示を出して、その都度内容を確認して、最終的な意思決定を上位者が行うのと同様に、子会社に対して本社が方針を示してモニタリングを行い、育成と意思決定に関与することが必要ではないでしょうか。逆に、ベテランの社員に対しては、業務を任せたと上で定期的に報告を受けるのと同様に、管理体制が成熟している子会社に対しては、権限を委譲して定期的に報告を受けるほうが効率的と考えられます。

4 第3線のアシュアランス活動

第1線と第2線のリスク管理体制と子会社第3線の成熟度を評価することで、第3線のアシュアランス活動の進め方を使い分けることが効果的です。子会社第3線（横軸）と子会社第1線と第2線のリスク管理体制（縦軸）の成熟度が共に高く、**図表2**の右上のケースに該当する場合には、子会社内部監査部の結果に依拠することを基本方針とします。一方、子会社内部監査部門の成熟度が低い場合には、依拠することが難しいため、本社内部監査部と共同監査を実施することで、監査品質の維持と子会社内部監査部の支援や育成に取り組みます。

また、第1線と第2線のリスク管理体制の成熟度が高い場合（縦軸）には、第2線を中心としたリスク管理体制の仕組みを監査することで効率化を図ることが可能と考えられます。一方、リスク管理体制が脆弱な場合には、個別にリスク評価を実施した上で、現場のプロセスやコントロールに対して監査手続きを実施することが必要となります。

図表2：第1線と第2線のリスク対応と第3線のアシュアランス活動

